

Форма № ДН-7.02.1

Державний вищий навчальний заклад  
«Донецький національний технічний університет»  
Кафедра Прикладної математики та інформатики



**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**  
**ОНД 2.11 ЗАХИСТ ОПЕРАЦІЙНИХ СИСТЕМ**  
(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність 125 Кібербезпека  
(шифр і назва спеціальності (тей))  
Освітня програма Кібербезпека  
(назва освітньої програми, для обов'язкових дисциплін)

Мова навчання: українська

Покровськ – 2021

Робоча програма навчальної дисципліни 125 Кібербезпека  
для здобувачів вищої освіти за спеціальністю 125 Кібербезпека

«27» січня 2021 року. – 8 с.

Розробник:  
Костін В.І., ст. викл. каф.ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики і інформатики  
(назва кафедри)

Протокол № 1 від. «28» січня 2021 р.

Завідувач кафедру ПМІ

«28» січня 2021 р

Схвалено науково-методичною комісією з галузі знань 12 Інформаційні технології  
(шифр, назва)  
Протокол № 1 від. «19» січня 2021 р.  
«19» січня 2021 р. Голова Башков Є.О.  
(підпис) (прізвище та ініціали)



## 1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	Вибіркова	
Обсяг в кредитах ЄКТС	5	
Обсяг в годинах за навчальним планом, разом:	150	
в тому числі:		
лекцій:	32	
практичні заняття:		
лабораторні заняття:	32	
семінари:		
самостійна робота:	86	
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Викладач І (Костін В.І., <a href="https://donntu.edu.ua/knt/pmi_valerii.kostin@donntu.edu.ua">https://donntu.edu.ua/knt/pmi_valerii.kostin@donntu.edu.ua</a> )	

**Передумови для вивчення дисципліни:** перелік дисциплін, які мають бути вивчені раніше: Програмування, Основи алгоритмізації, Основи інформаційної безпеки, Керування ризиками інформаційної безпеки, Чисельні методи, Аналіз випадкових процесів.

## 2. Мета вивчення навчальної дисципліни

**Мета:** Проведення інструментального моніторингу захищеності об'єкта; Розробка проектів систем і підсистем захищених операційних систем в Відповідно до технічного завдання; Пошук раціональних рішень при розробці засобів захисту інформації з урахуванням вимог якості, надійності і вартості, а також термінів виконання; Встановлення, настройка, експлуатація та обслуговування апаратно-програмних засобів захисту інформації; Забезпечення ефективного функціонування засобів захисту інформації з урахуванням вимог щодо забезпечення захищеності комп'ютерної системи.

### Компетентності:

- Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення (K13).
- Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування (K14)
- Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами (K16)
- Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних (K19).
- Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності загальної функціональності і надійності програмного забезпечення (K24)

- Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення (K25)
- Здатність до алгоритмічного та логічного мислення (K26)

### Програмні результати навчання:

- Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань (ПР13)
- Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення (ПР14);
- Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення (ПР19);
- Вміти застосовувати методи компонентної розробки програмного забезпечення (ПР17);
- Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних (ПР18);
- Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем (ПР21);
- ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
- ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
- ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
- ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
- ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

## 3. Очікувані результати навчання

Очікуваними результатами навчання є наявність у студентів навичок розробки програмних модулів, що реалізують завдання, пов'язані з забезпеченням безпеки операційних систем поширених сімейств; навичками оцінки рівня захисту операційних систем; засобами і



методами зберігання і передачі аутентифікаційної інформації; вимогами до підсистеми аудиту та політики аудиту; захисними механізмами і засобами забезпечення безпеки операційних систем; вмінні формувати і налаштовувати політику безпеки основних операційних систем, а також локальних комп'ютерних мереж, побудованих на їх основі; здійснювати заходи протидії порушенням безпеки з використанням різних програмних і апаратних засобів захисту; взаємодії різних операційних систем; класифікації програмного забезпечення мережних технологій; оцінці вартості програмного забезпечення в залежності від способу і місця його використання; адміністрування локальних обчислювальних мереж; вживання заходів щодо усунення можливих збоїв; встановлювати ОС; створювати і конфігурувати облікові записи окремих користувачів і груп користувачів; реєструвати підключення до домену;

#### 4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

- екзамени;
- розрахункові та розрахунково-графічні роботи;
- презентації результатів виконаних завдань та досліджень;
- виступи на наукових заходах.

#### 5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формувати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Оцінювання знань студента здійснюється за 100-бальною шкалою.

##### Для денної форми навчання

Поточний контроль							Поточний контроль	Іспит	Максим. сума балів
ЛР1	ЛР2	ЛР3	ЛР4	ЛР5	ЛР6	ЛР7			
3	3	6	7	7	7	7	40	60	100

Примітка: ЛР1, ЛР2 і т.д. практичні роботи;  
СЗ1, СЗ2 і т.д. семінарські заняття;  
ЛР1, ЛР2 і т.д. лабораторні роботи.

Схема оцінювання з урахуванням вимог Положення про організацію освітнього процесу. Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

## 6. Програма навчальної дисципліни

### 6.1 Основні теми дисципліни

**Тема 1.** Поняття захищеної операційної системи. Підходи до створення захищених ОС.

Адміністративні заходи захисту. Адекватна політика безпеки.

**Тема 2.** Механізми захисту ОС. Аналіз виконання сучасними ОС формалізованих вимог до захисту інформації от несанкціонованого доступу. Основні вбудовані механізми захисту ОС і їх недоліки.

**Тема 3.** Розмежування доступу до об'єктів ОС. Вимоги до правил розмежування доступу.

**Тема 4.** Ідентифікація, аутентифікація і авторизація користувачів ОС.

**Тема 5.** Інтеграція захищених операційних систем в захищену мережу. Переваги доменної архітектури локальної мережі.

**Тема 6.** Аудит в ОС. Необхідність аудиту. Вимоги до підсистеми аудиту. Політика аудиту. Організація аудиту.

**Тема 7.** Захист в операційній системі Unix

**Тема 8.** Захист в ОС Windows

### 6.2. Теми практичних (семінарських) занять

Не передбачено навчальним планом

### 6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	<b>Лаб робота 1.</b> Дослідження можливостей ОС по створенню облікового запису користувача з обмеженими правами	2	
2	<b>Лаб робота 2.</b> Дослідження порядку видалення обмеженого облікового запису	2	
3	<b>Лаб робота 3.</b> Дослідження засобів забезпечення безпеки облікових записів і розмежування доступу ОС Windows 10.	8	
4	<b>Лаб робота 4.</b> Дослідження засобів захисту від шкідливого ПО в ОС Windows 10.	4	
5	<b>Лаб робота 5.</b> Дослідження засобів відображення зовнішніх атак в ОС Windows 10.	6	
6	<b>Лаб робота 6.</b> Створення базової конфігурації в ОС Linux.	6	
8	<b>Лаб робота 7.</b> Вивчення підсистеми безпеки в ОС Linux.	4	
...	<b>Усього годин</b>	32	

### 6.4 Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	<b>Тема 1.</b> Поняття захищеної операційної системи. Підходи до створення захищених ОС. Адміністративні заходи захисту. Адекватна політика безпеки.	12	
2	<b>Тема 2.</b> Механізми захисту ОС. Аналіз виконання сучасними ОС формалізованих вимог до захисту інформації от несанкціонованого доступу. Основні вбудовані механізми захисту ОС і їх недоліки.	10	
3	<b>Тема 3.</b> Розмежування доступу до об'єктів ОС. Вимоги до правил розмежування доступу.	10	
4	<b>Тема 4.</b> Ідентифікація, аутентифікація і авторизація користувачів ОС.	12	



5	<b>Тема 5.</b> Інтеграція захищених операційних систем в захищену мережу. Переваги доменної архітектури локальної мережі.	12	
6	<b>Тема 6.</b> Аудит в ОС. Необхідність аудиту. Вимоги до підсистеми аудиту. Політика аудиту. Організація аудиту.	10	
7	<b>Тема 7.</b> Захист в операційній системі Unix	10	
8	<b>Тема 8.</b> Захист в ОС Windows	10	
	<b>Усього годин</b>	86	

#### 6.4. Індивідуальні та/або групові завдання (Не передбачено навчальним планом)

### 7. Література

#### 7.1 Основна

1. Основы защиты информации: учебное пособие. Изд. 5-е, перераб. и доп. – Томск: В-Спектр, 2011. – 244 с.
7. В.Г. Проскурин «Защита в операционных системах. Учебное пособие для вузов» М.: Гор. Линия-Телеком, 2014 – 192 с.
8. Проскурин В. Г. «Защита программ и данных: учеб. пособие для студ. учреждений высш. проф. образования» 2-с изд., — М. : Издательский центр «Академия», 2012. 208 с.
9. Макаренко С. И. Операционные системы, среды и оболочки: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2008. – 210 с.
10. Востокин С. В. «Операционные системы» учеб. - Самара: Изд-во Самар, гос. аэрокосм, ун-та, 2012. - 120 с.
11. А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. «Методы и средства защиты компьютерной информации : учебное пособие» – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.
12. Хорев П.Б. «Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. Заведений» — М.: Издательский центр «Академия», 2005. — 256 с.
13. Бакланов В.В. «Защитные механизмы операционной системы Linux: учебное пособие» - Екатеринбург: УрФУ, 2011. - 354 с.
14. В.Ю. Мельников, Е.К. Пугачев «Исследование методов защиты операционных систем и данных» -Московский государственный технический университет имени Н.Э. Баумана 2017 – 100 с.

#### 7.2 Допоміжна

Модель безопасности ОС Windows. Методические указания к лабораторным работам по курсу «Защита информации» - Волгоград 2011 – 24 с.  
Авраменко В.С., Авраменко А.С. «Основы операционных систем. Навчальний посібник». – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524с.

#### 7.3 Методична

1. Методичні вказівки та завдання к лабораторним роботам по курсу «Захист операційних систем», (в розробці)

### 8 Інформаційні ресурси

1. [https://zinref.ru/000\\_uchebniki/02800\\_logika/011\\_lekcii\\_raznie\\_33/1562.htm](https://zinref.ru/000_uchebniki/02800_logika/011_lekcii_raznie_33/1562.htm)
2. <https://rutd-ksk.com/shtatnye-sredstva-zaschity-informatsii-v-operatsionnyh-sistemah/>
3. <http://all-light.narod.ru/apzci/apzci.htm>
4. <http://temowind.ru/bezopasnost-windows-7/sposoby-zashhity-operacionnyx-sistem/>
5. [http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2016/01/BOSM\\_03\\_2015.pdf](http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2016/01/BOSM_03_2015.pdf)